Special Publication 800-73: Interfaces for Personal Identity Verification

Jim Dray

PIV Implementer's Workshop

June 27, 2005

SP800-73 Structure

- Part 1: Architectural model
- Part 2: Transition specification
- Part 3: Endpoint specification

NIST
National Institute of Standards and Technology

Part 1

- Migration issues
  - Part 2 provides an informative transition path for agencies with legacy card deployments
  - Part 3 is the mandatory endpoint specification
- Common Data Model
  - Common to both Part 2 and Part 3 specifications

NIST
National Institute of Standards and Technology

Common Data Model

- Mandatory elements:
  - card capability container
  - cardholder unique identifier (CHUID, ref PACS)
  - fingerprints (2)
  - security object
- Optional elements:
  - printed information
  - facial image
  - digital signature certificate
  - key management certificate
  - card authentication certificate

NIST National Institute of Standards and Technology

Part 2 (I)

- Based on GSC-ISv2.1 (NISTIR 6887 2003)
- Developed by the GSC Interagency Advisory Board
- Basic Services Interface
- 2-byte GSC-IS ‘object identifiers’ embedded in AID (PIX of RID)
  - container = card application
- ‘Hard’ file system and VM card edges
  - No APDU mapping

NIST
National Institute of Standards and Technology

Part 2 (II)

- Only a subset of GSC-IS APDUs are used
- Differences from GSC-IS:
  - SELECT – CCC retrieval
  - VERIFY – PIN format
  - PRIVATE SIGN/DECRYPT- Chaining

Part 3: Overview

- Unified card edge
- Technology neutral
- Standards compliant
- Standard PIV namespaces
- Simple PIV card application specification to support FIPS 201 requirements

NIST
National Institute of Standards and Technology

Part 3: Functionality

- Read CHUID (physical access control)
- Retrieve biometric objects (PIN protected) for off-card matching
- Retrieve public key certificates
- Challenge-response authentication (PKI)
- Optional card authentication, key management, digital signature generation

NIST
National Institute of Standards and Technology

Part 3: Components

- Common Data Model
- Client API
- Card Interface
- Security Model

NIST
National Institute of Standards and Technology

Part 3: Namespaces

- PIV Registered Application Provider Identifier = ‘A0 00 00 03 08’
  - PIX contains versioning information
- OIDs at the client API
  - PIV arc of the Computer Security Object Register managed by NIST
- BER-TLV at the card interface
  - Hardwired mapping to OIDs

NIST
National Institute of Standards and Technology

Part 3: Client API (I)

- Equivalent to GSC-IS BSI
- Part 3 middleware is much simpler than GSC-IS due to elimination of APDU mapping mechanisms
- GSC-IS manages the differences between cards below the client API. Part 3 makes all PIV cards functionally identical at the card interface, eliminating the need for this middleware management function.

NIST
National Institute of Standards and Technology

Part 3: Client API (II)

- pivConnect
- pivDisconnect
- pivSelectCardApp
- pivLogIntoApp
- pivGetData
- pivLogoutOfApp
- pivCrypt
- pivPutData
- pivGenerateKeyPr

NIST
National Institute of Standards and Technology

Part 3: Card Interface

- SELECT
- GET DATA
- VERIFY
- CHANGE REFERENCE DATA
- RESET RETRY COUNTER
- GENERAL AUTHENTICATE
- PUT DATA
- GENERATE ASYMMETRIC KEY PAIR

Part 3: Security Model

- Access Control Rules
  - Access mode: Operation on a data object
  - Security condition: Boolean combination of security status indicators
    - Security status indicators are associated with each entity that can authenticate to the card
    - Can be global or local to the PIV application
- Example: The cardholder's PIN must be verified prior to reading a biometric object

NIST
National Institute of Standards and Technology

Part 3: Architectural Model

- Default application
  - May or may not be PIV application
  - Truncated AID may be used for selection
- On-card format of data objects not specified
  - Format is only specified at the interface level
  - Objects are treated as ‘blobs’ to be parsed at application layer
  - Allows dynamic construction of objects

PIV Card Management

- GSC-IAB Policy Group recommendation
  - No requirement for interoperability of card management systems across agencies
  - Common initial state for mandatory data objects
- Some ‘credential initialization and administration’ hooks included
- NIST is initiating a PIV card management study for informative purposes

NIST
National Institute of Standards and Technology

Summary

SP 800-73 Part 3 specifies a PIV card application that is straightforward to implement, technology neutral, and standards compliant. The PIV namespaces are internationally recognized and tightly managed by NIST to assure a high level of interoperability in the PIV domain. NIST has undertaken several activities to facilitate development of PIV products including publication of a reference implementation, creation of a PIV conformance test program, and a card management study.

NIST
National Institute of Standards and Technology

Contact Details

james.dray@nist.gov: GSC Chief Architect

teresa.schwarzhoff@nist.gov: GSC Standards Program Manager

william.barker@nist.gov: PIV Project Manager

PIV Website: http://csrc.nist.gov/piv-project

NIST
National Institute of Standards and Technology